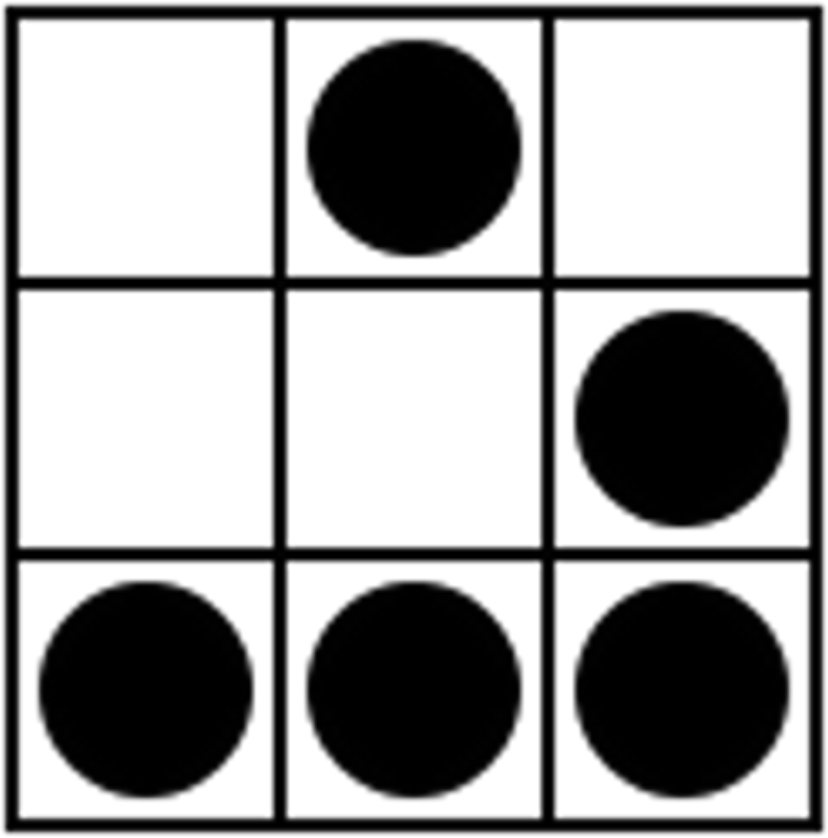
Guide To
Cyber Security



Written By

David Childers

www.ScenicRadio.Com

Relaxing Entertainment for the World

www.BroadcastingWorld.Com

Global Broadcast Information Portal

Cover graphic - A "glider" from Conway's Game of Life.
en.wikipedia.org/wiki/File:Glider.svg

Foreword graphic - Een geleerde in zijn werkkamer
en.wikipedia.org/wiki/File:Rembrandt,_Faust.jpg

About The Author

David Childers is the Content Manager for the Global Broadcasting portal www.BroadcastingWorld.com. He is very active in the Internet broadcast industry and has written numerous guides and a book about this growing technological field. He is also the webmaster of www.ScenicRadio.com, the global destination for relaxing entertainment.

Mr. Childers' work has been cited in several national and International publications, including these:

Five Essays on Copyright In the Digital Era
Turre Publishing

Research On High-Profile Digital Video Production
Digital Content Association of Japan

Video Podcasting in Perspective: The History, Technology, Aesthetics and Instructional Uses of a New Medium
Journal of Educational Technology Systems

Video Podcasting: When, Where and How it's Currently used for Instruction
The National Convention of the Association for Educational Communications and Technology

IP Packet Charging Model For Multimedia Services
National University of Rwanda

Preservation of audiovisual mediums: Problems and challenges
Platform for Archiving and Preservation of Art on Electronic and Digital Media

P2P Technology Trend and Application to Home Network
Electronics and Telecommunications Research Institute Journal

Peer To Peer Computing - The Evolution of a Disruptive Technology
Idea Group Publishing

Peer-to-Peer Systems and Applications
Lecture Notes In Computer Science
Springer Berlin / Heidelberg

Feedback

Please feel free to contact the author if you have any questions or comments. Your feedback is greatly appreciated.

You can contact the author here: www.KL7AF.com

Foreword

Welcome to another glimpse into the realm of knowledge.

Computer system and data network security is very important in view of the constant attacks by rogue computer operators and hacker groups. Every computer user should take great care in maintaining their computer and when accessing public data networks such as the Internet. Malware or attacks on a system can quickly turn any computer into a remotely controlled zombie. Knowledge and planning can prevent security problems from happening.

The musical inspiration for this guide is Nightmares On Wax – Les Nuits, Original Mix.

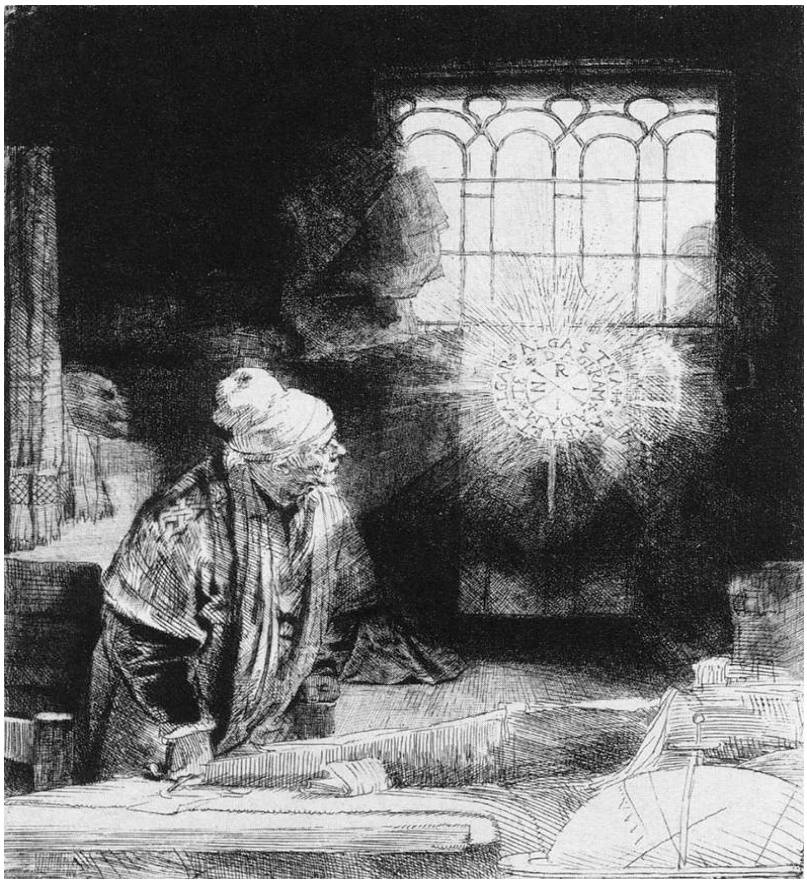
I would like to thank Scarlet Coker for providing assistance with the editing of the manuscript and James Davey at Broadcasting World for allowing me the opportunity to create this guide.

It is my sincere hope that the reader finds this guide beneficial.

David Childers

June 2012

Posveèeno Neži Vidmar.



Minima Maxima Sunt.

Better be despised for too anxious apprehensions, than ruined by too confident security.

Edmund Burke

Index

Introduction

It is important to guard against computer system or data network misuse or trespassing. Prevention of these security threats can be achieved through the use of active or passive methods. Each of these methods can be used individually or integrated together to achieve a greater standard of security.

Protecting a computer system or network against vulnerabilities is never a one step procedure, it must be a continuing process for both the computer administrator and individual computer user. Both individuals must incorporate thorough security practices and stay informed of current security issues and vulnerabilities.

Security risks can come from various sources, which include:

- Failure to properly maintain computer system software.

- Installing comprised software.

- Using compromised computer systems.

- Accessing compromised websites.

- Lack of physical security for computer systems.

- Lack of network security for computer systems.

Knowledge and vigilance are the keys to maintaining security.

System Core

The central component of a computer operating system is known as the kernel. This component manages system resources in addition to coordinating data flow between installed software and system hardware.

Unmodified kernels are fairly robust and can usually withstand outside attacks that attempt to alter or control the internal operation. Some operating system kernels can be modified to increase their overall security. Each operating system has special requirements for kernel operation and these should be carefully examined. Kernel modification requirements can range in complexity and skills needed.

It is important to use extreme caution when modifying or reconfiguring a kernel. If proper modification procedures are not followed errors, system instability, acute system vulnerability or data loss can occur. Kernel modifications are usually permanent and should be validated when the operating system is updated or refreshed. Any modifications made to the kernel should be fully documented and the information retained. This information can be useful in diagnosing problems if they occur in the future.

System Passwords

Passwords are usually the weakest link in computer system security. The purpose of a password is to prevent unauthorized people from gaining access to a computer or data network. Using simple or common words for passwords is the equivalent of not using any password protection.

- Select strong passwords for the ADMINISTRATOR login. This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Select strong passwords for the USER login. This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Document all password information.

- Maintain physical security of password information.

- Do not store system passwords on the computer.

  *** Post it notes invite trouble.**

- Do not use identical passwords for system account logins.

  * Administrator – Different password

  * User – Different password

- Establish a set routine for changing ALL system passwords on a regular basis.

  * Administrator

  * User

System Accounts

Computer systems generally have two types of system access accounts. These consist of an administrator and user accounts.

The administrator account has complete access and control over the entire computer system. This account can install software or make system configurations that affect the overall function of the computer system. Administrator accounts should only be used to install software used on a system wide basis or make system configurations for all users.

General work should be done using the user account. Each individual on a computer system can configure their own user account to suit their personal needs, without changing system wide configuration. This can prevent situations that would affect the entire system.

Any errors that may occur in the course of work being undertaken in a user account will affect only the individual user account settings and not make system wide changes. If a user account has been corrupted or misconfigured, it can be deleted with no significant damage done to the complete system.

System Monitoring

Monitoring computer system activity and system logs can provide an indication of system, hardware or software trouble. This ability can also indicate the possible existence of security problems or issues within the system.

Real time monitoring of the computer system can provide an immediate indication of possible system problems.

- Unusual activity that could indicate trouble includes:

  * Excessive CPU use.

  * Excessive RAM use.

  * Excessive hard drive use.

  * Excessive connections to computer.

  * Sluggish system response.

  * Slow network response time.

- Monitoring of the computer system logs can provide a documented indication of possible system problems.

  * Hardware fault.

  * Software fault.

  * Network fault.

System Software

It is important to maintain operating system and application software updates and patches. This will prevent system instability and possible security problems.

Operating system software maintenance allows the computer to properly function. These upgrades prevents problems from occurring or existing problems to be fixed.

- Ensure that the operating system is kept up to date.

* It is extremely important to install patches and updates to the computer operating system on a regular basis; especially critical updates.

- Subscribe to the computer operating system's announcements list for security or maintenance issues.

- Periodically check the computer operating system's website for security or maintenance issues.

System security notifications

Official points of information for major operating systems:

Linux Redhat Security
access.redhat.com/security/updates

Linux Fedora Security
lists.fedoraproject.org/mailman/listinfo/security

Linux Debian Security
lists.debian.org/debian-security-announce/

Linux Ubuntu Security
www.ubuntu.com/usn

Linux OpenSUSE Security
en.opensuse.org/Portal:Security

OpenBSD Security
www.openbsd.org/security.html

FreeBSD Security
security.freebsd.org

NetBSD Security
www.netbsd.org/support/security/advisory.html

Apple Security
ssl.apple.com/support/security/

Windows Security
technet.microsoft.com/en-us/security/bulletin

Software maintenance allows the installed applications to properly function. These upgrades prevents problems from occurring or existing problems to be fixed.

- Ensure that all application software is kept up to date.

* Install patches and upgrades immediately upon notification.

- Subscribe to the application software's announcements list for security or maintenance issues.

- Periodically check the application software's website for security or maintenance issues.

Do not install application software that can allow unauthorized remote users to access the computer or allow malicious software to modify the computer system.

THINK BEFORE YOU CLICK OR INSTALL.

It is important to research information about software applications and ensure that they are valid, rather than having

to re install the entire operating system and all needed applications.

General software announcements

Cyber Security Current Bulletins
www.us-cert.gov/current

Cyber Security Alerts
www.us-cert.gov/cas/techalerts/index.html

Cyber Security Bulletins Listing
www.us-cert.gov/cas/bulletins

System Firewall

A firewall is an application that prevents unauthorized remote access to a computer, which is achieved by securing system communication ports. These communication ports are used by the computer system to exchange data with other computer systems when it is connected to data networks.

It is very important to ensure the firewall is configured properly. A firewall that is not correctly configured provides marginal security benefit to the host computer.

Common computer communication ports

This is a list of common communication ports employed by computer systems used on data networks.

Additional communication ports may be used by other installed software applications. It is important to check the software application documentation to correctly configure the firewall.

20 File Transfer Protocol - Data transfer.

22 Secure Shell - For secure logins, file transfers and port forwarding.

23 Telnet - Unencrypted text communications.

25 Simple Mail Transfer Protocol - For e mail routing between mail servers.

37 TIME protocol.

80 Hypertext Transfer protocol.

115 Simple File Transfer protocol.

123 Network Time protocol - System time synchronization.

443 Hypertext Transfer Protocol over Transport Layer Security or Secure Sockets Layer.

513 Remote login.

514 Shell - For executing non-interactive commands on a remote system.

563 Network News Transfer protocol over Transport Layer Security or Secure Sockets Layer.

989 File Transfer Protocol Secure (data): Data transfer over Transport Layer Security or Secure Sockets Layer.

990 File Transfer Protocol Secure (control): Data transfer over Transport Layer Security or Secure Sockets Layer.

Once the firewall is installed and configured, a scan of the computer system communication ports should be conducted. This will verify that the firewall has been properly configured and is working correctly.

Free online port scan and firewall testing

www.auditmypc.com/firewall-test.asp

www.securitymetrics.com/portscan.adp

www.grc.com/x/ne.dll?bh0bkyd2

Data Management

Protecting and backing up system data provides the ability to restore system operation if the integrity of the hardware or software has failed. This can also prevent personal or sensitive information from being accessed if the computer system has been compromised.

- Routinely encrypt sensitive or personal data.

- Back up important computer system files on a routine basis.

- Back up computer application software installation media.

- Keep all important hardware and software documentation together.

- Keep all login information secure.

- Store computer back up data on removable media.

- Store software back up data on removable media.

Malware

Malicious software (generally known as malware), is software intentionally designed to disrupt a computers operation, gather sensitive information from it, or gain unauthorized access to it. Malware can also appear in the form of scripts or html code embedded on websites or within software applications. Malware includes computer trojans, viruses, adware, worms, spyware, rootkits, and other forms of malicious computer programs.

It is very important to properly configure a computer system to thwart infection or contamination by malware. The old saying “An ounce of prevention is worth a pound of cure,” (Benjamin Franklin), rings true on how planning can impede disasters in the future.

It is important to create a plan and use the proper applications to block malware infection or contamination of a system. This plan and associated software should include the following criteria:

- Prevention.

- Detection.

- Containment.

- Eradication.

Wireless

Wireless data communications can be useful for accessing data in a mobile setting. It can also be a security nightmare for both the end user and wireless network administrator. Attention to detail and vigilance is a must for ensuring network and data integrity.

Wireless encryption key password recommendation

- Change the default password setting for the encryption key used by the wireless network router.

- This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Establish a routine for changing the encryption key password for the wireless network router.

- It is vital that any password information is documented and stored in a secure method.

- DO NOT USE ANY DEFAULT PASSWORD SETTING.

Wireless router administration password recommendation

- Change the default password setting for the administrator access to the wireless network router.

- This password should contain a minimum of 15 characters, that should include at least 2 upper case letters, 2 lower case letters, 2 numbers and two special characters.

- Establish a routine for changing the administrative password for the wireless network router.

- It is vital that any password information is documented and stored in a secure method.

- DO NOT USE ANY DEFAULT PASSWORD SETTING.

Safeguard wireless network password information

It is important to educate and inform all persons that access a business or organizational wireless network that they must safeguard the network access password information. It is imperative they understand the wireless network can be compromised and valuable data can be lost if they misuse this information.

SSID (Service Set Identifier)

This is a broadcast that indicates the identification and presence of a wireless network router. Turning off the SSID feature will disable the ability of people to casually detect the presence of a wireless network router.

DO NOT USE ANY DEFAULT SSID IDENTIFICATION SETTINGS. The SSID identification should contain both numbers and letters, in addition to using a minimum of 8 letters for the identification. It is highly recommended that ordinary phrases or names are not used for the SSID.

Additional data encryption

Using additional data network encryption provides a second layer of security in addition to the encryption processes used by the wireless network. This can be utilized between a wireless connected client and a encryption service provider. This also provides data security when using open, public or non encrypted wireless network access points.

Virtual Private Networks

This networking technology encrypts data exchanged between remotely located computer systems. Advanced cryptographic methods are used to encode the data, which prevents it from being analyzed or monitored by third parties while it is being exchanged.

The use of Virtual Private Networks can also prevent personal or private data from being accessed on open or closed wireless networks.

VPN Tools

Proxpn

(Free and paid service available.)

www.proxpn.com

Securitykiss

(Free and paid service available.)

www.securitykiss.com

Secure Socket Layer

This is a cryptographic protocol that provides additional security for communications over the Internet. This encrypts data between a remote computer and a website. This type of Internet communication is characterized by the inclusion of a **S** following the **HTTP** URL designator.

Example: **HTTPS**://www.google.com

Secure Socket Layer Tools

HTTPS Everywhere

A Firefox extension that provides encrypted computer network communications with a number of major websites.

www.eff.org/https-everywhere

Linux Software

System Core

AppArmor

Open source security module for the Linux kernel.

wiki.apparmor.net/index.php/Main_Page

Tomoyo

Open source security module for system analysis and protection.

tomoyo.sourceforge.jp/index.html.en

Grsecurity

Open source Linux kernel patches with an emphasis on enhancing security.

www.grsecurity.net

Security-Enhanced Linux

Open source add on that provides a mechanism for supporting access control security policies.

www.nsa.gov/research/selinux/

System Passwords

Passgen

Open source GUI password generator.

sourceforge.net/projects/passgengui/

High-Security Offline Password Generator

Open source command line password generator.

www.defuse.ca/passgen.htm

System Monitoring

Devilish

Open source PyGTK application for monitoring Linux log files in realtime.

github.com/iye/Devilish

Conky

Open source light weight system monitor for X.

conky.sourceforge.net/index.html

Monit

Open source utility for managing and monitoring, processes, programs, files, directories and file systems.

www.mmonit.com/monit/

GKrellM

Open source GTK based stacked monitor program that charts SMP CPUs, disks, load, active net interfaces, and internet connections.

www.freecode.com/projects/gkrellm

System Firewall

Firewall Builder

Open source graphic user interface for configuring firewalls.

www.fwbuilder.org

Firestarter

Open source GUI firewall.

www.fs-security.com

Data Management

True Crypt

Open source application used for on the fly encryption for hard drives.

www.truecrypt.org

TestDisk

Open source data recovery application.

www.cgsecurity.org/wiki/TestDisk

Ddrescue

Open source data recovery tool.

www.gnu.org/software/ddrescue/ddrescue.html

Safecopy

Open source data recovery application that can be used on damaged media.

safecopy.sourceforge.net/

Areca Backup

Open Source personal backup solution.

www.areca-backup.org

BackupPC

Open source high-performance backup application.

backuppc.sourceforge.net

fwbackups

Open source feature rich user backup program.

www.diffingo.com/oss/fwbackups

extundelete

Open source utility that can recover deleted files from an ext3 or ext4 partition.

extundelete.sourceforge.net

Malware

Clam AV

Open source anti virus engine designed for detecting Trojans, viruses, malware and other malicious threats.

www.clamav.net

Linux Malware Detect

Open source malware scanner.

www.rfxn.com/projects/linux-malware-detect/

Nessus

A closed source comprehensive computer vulnerability scanning program.

This software is also available in various distributions software repositories.

www.tenable.com/products/nessus

OpenVAS

Open source vulnerability scanner and manager.

www.openvas.org

Snort

Open source network intrusion prevention and detection system.

www.snort.org

Suricata Engine

Open source next generation intrusion detection and prevention system.

www.openinfosecfoundation.org/index.php/download-suricata

Wireless

Wavemon 802.11 Monitor

Open source ncurses based comprehensive monitoring application for 802.11 wireless network devices.

eden-feed.erg.abdn.ac.uk/wavemon/

Network Traffic

Guardster

Free web proxy service that provides anonymously web browsing and privacy.
Can also be used to circumvent restrictions on website access.

www.guardster.com/free/

Hide My Ass

Free web proxy service that provides anonymously web browsing and privacy.
Can also be used to circumvent restrictions on website access.

www.hidemyass.com

Tor

Software that enables online anonymity.

www.torproject.org

DNSCrypt

Encrypts DNS (Domain Name Service) traffic to prevent eavesdropping and man-in-the-middle attacks.
For use with OpenDNS service. (Free)

www.opendns.com/technology/dnscrypt/